

RENFORCEZ, **VOTRE SÉCURITÉ**

avec Fellowes



Comprendre le **RGPD** et la directive **NIS-2**
et intégrer la protection des données dans
votre quotidien professionnel.

Fellowes

INTRODUCTION

Pourquoi la protection des données est plus importante que jamais ?

Dans un monde de plus en plus connecté, exposé aux cybermenaces et aux atteintes à la vie privée, la protection des données n'est plus une option. Protéger les données de votre entreprise est essentiel et assurer la conformité aux lois sur la protection des données est plus important que jamais.

La mise à jour des réglementations RGPD et NIS-2 oblige les entreprises à protéger les données sensibles et personnelles de manière responsable qu'elles soient physiques ou numériques. Le non-respect de ces obligations peut entraîner de lourdes amendes, nuire à la réputation et engager la responsabilité personnelle des dirigeants.

Ce guide fournit un aperçu des deux réglementations, afin de vous aider à comprendre vos obligations et à prendre des mesures pour assurer votre conformité.



***Renforcez votre sécurité.
Protégez votre entreprise.
Restez en conformité.***



Connaissez-vous les données personnelles ?

Les données personnelles sont toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, par exemple :



Noms



Adresses



**Numéros de
sécurité sociale**



**Images de
vidéosurveillance (CCTV)**

**Protéger les données
signifie protéger à la fois
les informations numériques
et papier, une violation de
données peut survenir sous
l'une ou l'autre de ces formes.**

QU'EST-CE QUE NIS-2 ?

Renforcer la cybersécurité en Europe

La directive sur la sécurité des réseaux et de l'information (NIS-2) est la plus récente législation de l'UE visant à améliorer la cybersécurité et la résilience des secteurs critiques. Entrée en vigueur en 2023, elle doit être transposée par l'ensemble des États membres de l'UE depuis octobre 2024.

La directive NIS-2 reconnaît que les économies modernes reposent sur l'infrastructure numérique et que les perturbations liées à des incidents cybernétiques peuvent avoir des conséquences dévastatrices. Elle s'applique ainsi aux entités dites "essentielles" ainsi qu'aux entités "importantes".

NIS-2 s'applique-t-elle à votre entreprise ?

Si votre organisation joue un rôle clé dans l'économie ou la société, même indirectement, il est probable qu'elle relève de NIS-2. La directive s'applique aux produits et services classés comme secteurs « essentiels » ou « importants ».

Entités essentielles :



Énergie



Transport



Infrastructures
numériques



Banques



Infrastructures de
marché financier



Eau potable



Gestion des tic



Administration
publique



Espace



Eaux usées



Santé

Entités importantes :



Services postaux
et de messagerie



Gestion des
déchets



Fabrication



Production
chimique



Recherche



Production
alimentaire



Fournisseurs
numériques

Les deux principes de NIS-2

Les entreprises relevant de NIS-2 doivent mettre en place des mesures préventives et des mécanismes de réponse.



Devoir de diligence (Duty of Care) :

les organisations doivent mettre en œuvre des mesures techniques, opérationnelles et organisationnelles proportionnées pour assurer la sécurité numérique et la continuité. Cela peut inclure la sécurisation des systèmes informatiques, l'évaluation des vulnérabilités, la gestion des risques liés à la chaîne d'approvisionnement et la responsabilité au niveau de la direction.




Obligation de notification (Duty to Report) :

les organisations doivent notifier les autorités nationales compétentes en cas d'incidents significatifs. Les interruptions majeures doivent être signalées sous 24 heures, les autres incidents sous 72 heures. Un rapport final détaillé doit être soumis dans un délai d'un mois.

Sanctions en cas de non-conformité :

Le non-respect de NIS-2 peut entraîner de lourdes conséquences financières et opérationnelles :

AMENDES  
Jusqu'à
10 millions €
ou 2% du chiffre d'affaires
annuel mondial pour les
entités essentielles

AMENDES  
Jusqu'à
7 millions €
ou 1,4% du chiffre d'affaires
annuel mondial pour les
entités importantes

Les dirigeants peuvent être tenus personnellement responsables, y compris avec des interdictions temporaires ou permanentes d'exercer dans certains secteurs.

Le risque caché : les violations de données papier

Bien que NIS-2 se concentre sur la résilience numérique, les risques liés aux données physiques ne doivent pas être négligés. Tout incident où des données personnelles sont perdues, volées ou divulguées de manière inappropriée est concerné, y compris lorsqu'il s'agit de documents papier non détruits de manière sécurisée. Pensez à des contrats jetés dans une corbeille, des feuilles de calcul laissées sur des bureaux, des dossiers RH dans des armoires non verrouillées ou des factures dans des bacs de recyclage accessibles. Chacun de ces scénarios peut exposer votre entreprise à des sanctions financières et porter atteinte à votre réputation.

QU'EST-CE QUE LE RGPD ?

Protéger les données personnelles

Le Règlement général sur la protection des données (RGPD) régit depuis 2018 la protection des données dans l'UE et au Royaume-Uni. Il garantit que les données personnelles soient traitées légalement, de manière transparente et sécurisée.

Les 6 principes de la protection des données

Ces six principes doivent constituer le cœur de toute stratégie de protection des données. Les données doivent être :

1. Traitées de manière licite, loyale et transparente.
2. Collectées pour à des fins déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités initiales.
3. Adéquates, pertinentes et limitées à ce qui est nécessaire.
4. Exactes et tenues à jour ; les inexactitudes doivent être corrigées, effacées ou rectifiées sans délai.
5. Conservées pendant une durée n'excédant pas celle nécessaire.
6. Traitées en toute sécurité.

Quand faut-il signaler une violation de données ?

Les violations doivent être signalées aux autorités dans les 72 heures et, dans certains cas, aux personnes concernées.



Sanctions en cas de non-conformité :

Le non-respect du RGPD peut entraîner de lourdes conséquences financières :

AMENDES
Jusqu'à



20 millions €

ou 4% du chiffre d'affaires mondial,
selon le montant le plus élevé

NIS-2 vs RGPD

Comprendre les différences

En résumé, voici un aperçu comparatif des deux réglementations distinctes :

ASPECT	NIS-2	RGPD
Objectif	Cybersécurité et résilience numérique dans les secteurs essentiels et importants.	Protection des données personnelles (numériques et papier) pour toutes les organisations traitant des données des citoyens UE/UK.
Champ d'application	Entités essentielles et importantes (énergie, transport, banques, santé, infrastructures numériques, etc.).	Toute organisation collectant, stockant ou traitant des données personnelles.
Principes clés	Devoir de diligence & obligation de notification.	Six principes de protection des données (licéité, limitation des finalités, minimisation des données, exactitude, limitation de conservation, intégrité et confidentialité).
Signalement des incidents	Aux autorités dans les 24 h pour perturbation, 72 h pour autres cas.	Aux autorités dans les 72 h, parfois également aux personnes concernées.
Sanctions	Jusqu'à 10 M € ou 2 % C.A (entités essentielles), jusqu'à 7 M € ou 1,4 % C.A (entités importantes).	Jusqu'à 20 M € ou 4 % du C.A mondial.
Responsabilité des dirigeants	Responsabilité personnelle possible, interdiction d'exercer dans certains secteurs.	Organisation sanctionnée, responsabilité pouvant concerner DPO ou managers.

Actions pratiques

Renforcer la conformité

Pour la plupart des organisations, se conformer à NIS-2 et au RGPD implique de combiner des politiques solides, une technologie sécurisée et la sensibilisation quotidienne des employés.

1 Vérifier vos obligations

Vérifier si votre organisation est classée comme entité essentielle ou importante sous NIS-2.

Revoir vos responsabilités RGPD et comprendre quelles données vous détenez et pourquoi.

2 Renforcer les pratiques de sécurité

Mettre en œuvre et mettre à jour régulièrement les pare-feu, le chiffrement et les plans de réponse aux incidents.

Ne pas négliger les risques physiques – contrôle des impressions non surveillées, archivage et destruction sécurisée.

3 Définir les procédures de notification

Établir des chemins clairs d'escalade pour les incidents.

Désigner un responsable chargé du signalement et de la documentation des violations.

S'assurer que l'équipe est en mesure de respecter les délais réglementaires de notification (24-72 h).

4 Former régulièrement les employés

Faire de la protection des données une culture quotidienne, pas seulement une politique de la charte informatique.

Couvrir à la fois les risques numériques (phishing, gestion des mots de passe) et papier (stockage, destruction).

5 Contrôler le cycle de vie des documents

Introduire une politique de destruction pour les documents papier obsolètes.

Conserver les documents sensibles en toute sécurité jusqu'à leur destruction.

Ne conserver que ce qui est nécessaire, revoir les archives régulièrement et détruire les fichiers expirés en toute sécurité.

Solutions Fellowes

Outils pratiques pour renforcer la conformité

De la destruction sécurisée à l'archivage organisé et aux filtres de confidentialité pour écran, les solutions Fellowes vous aident à protéger l'information à chaque étape de son cycle de vie, soutenant vos efforts pour rester conforme aux directives NIS-2 et RGPD.

Votre problématique :

Prévenir les fuites de données à partir de documents papier

Notre solution

Destructeurs - Intégrer la destruction dans la politique documentaire réduit le risque de fuite. Détruisez les copies papier inutiles afin que les données sensibles ne puissent pas être récupérées ou utilisées à mauvais escient.

[Découvrez nos destructeurs de documents](#)



Votre problématique :

Stocker les dossiers physiques de manière sûre et systématique

Notre solution

Solutions d'archivage - Maintenez vos archives organisées avec les produits BANKERS BOX® clairement étiquetés et bien organisés pour un transport sécurisé jusqu'à la destruction.

[Découvrez nos solutions de classement et d'organisation](#)



Votre problématique :

Protéger les données affichées à l'écran contre les regards indiscrets

Notre solution

Filtres de confidentialité - Ils empêchent le vol visuel de données affichées à l'écran. C'est une solution idéale pour les travailleurs hybrides et les environnements de bureaux partagés.

Découvrez les filtres de confidentialité

PrivaScreen™.

Votre problématique :

Sécuriser vos appareils en déplacement ou dans les espaces partagés

Notre solution

Mallette de rangement ergonomique - La mallette Breyta™ deux-en-un verrouillable protège l'ordinateur, les documents importants et les accessoires et sert également de support pour ordinateur portable.

Découvrez la gamme Breyta™





La protection des données n'est plus seulement une responsabilité IT !
C'est un engagement à l'échelle de l'organisation. En alignant votre entreprise sur le RGPD et NIS-2 et en intégrant des pratiques sûres de gestion des documents et des données au quotidien, vous pouvez éviter les amendes, renforcer la confiance et accroître votre résilience.

**Intégrez la protection des données dans
votre quotidien professionnel.**

Fellowes
Brands™

ENTREPRISE FAMILIALE
DEPUIS 1917

www.fellowes.com